NAVAL WAR COLLEGE
Newport, R.I.

U.S. Space Command's Role in Computer Network Defense: 2020 Vision or Hack Job?

By

Scott A. Stephenson

Commander, United States Navy

A paper submitted to the Joint Military Operations Faculty in partial satisfaction of the requirements for the Master of Arts Degree in National Security and Strategic Studies.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature:_____

13 May 2002

Faculty Advisor
Erik J. Dahl
Commander, USN

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED

2. Security Classification Authority:

3. Declassification/Downgrading Schedule:

4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

5. Name of Performing Organization:
JOINT MILITARY OPERATIONS DEPARTMENT

6. Office Symbol: C

7. Address: NAVAL WAR COLLEGE
686 CUSHING ROAD
NEWPORT, RI 02841-1207

8. Title (Include Security Classification):

U.S. Space Command's Role in Computer Network Defense:2020 Vision or Hack Job?

9. Personal Authors:
CDR Scott A. Stephenson

10.Type of Report: FINAL

11. Date of Report: 13 May 2002

12.Page Count:

12A Paper Advisor (if any): CDR Erik J. Dahl

13.Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. Ten key words that relate to your paper:

Information Security, Computer Network Defense, Defense in Depth, Computer Network Attack

15.Abstract: The UCP change that assigned responsibility for CND to U.S. Space Command (USSC) is a fundamentally flawed attempt to correct a perceived deficiency in Information Operations (IO) doctrine and organizational design. The CND mission has been defined too narrowly and rigidly and will result in the introduction of exploitable vulnerabilities in the Defense Information Infrastructure (DII). These DII vulnerabilities will be easily and quickly exploited by sophisticated adversaries in a manner that is imperceptible to those charged with protecting it. USSC will not and cannot be effective in improving the integration of CND into military planning and operations. On the contrary, it will likely slow development and fielding of new defensive capabilities, unnecessarily complicate inter-service and inter-agency coordination, and potentially weaken the U.S. military's information security posture.

16.Distribution / Availability of Abstract:	**Unclassified**	**Same As Rpt**	**DTIC Users**
	X		

17.Abstract Security Classification: UNCLASSIFIED

18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19.Telephone: 841-3556	**20.Office Symbol:** **C**

Security Classification of This Page Unclassified

Introduction

> DoD is betting the farm on having assured information in its information networks, now collectively referred to as the Global Information Grid (GIG). The GIG is a fundamental tenet of the Department's Joint Vision 2020. Without a considerable effort to provide information assurance, such a complex system will introduce inherent, and perhaps crippling, vulnerabilities into the military force structure.
>
> ---- Defense Science Board Task Force on Defensive Information Operations – 2000 Summer Study.[1]

Computer Network Defense (CND) is critically important to the Joint Vision 2020 concept of Full Spectrum Dominance and its operational components of dominant maneuver, precision engagement, full dimensional protection, and focused logistics. Specifically, CND is a critical underpinning of Joint Vision 2020's key enabler, Information superiority. The DoD's strategic vision for the 21st century is to ensure that U.S. forces have information superiority in every mission area and to provide all of DoD's customers with assured and secure connectivity on a protected global network. Information superiority is the capability to collect, process, and disseminate an uninterrupted flow of information while denying an adversary's ability to do the same.[2] It is the backbone of the Revolution in Military Affairs known as Network Centric Warfare (NCW) and provides comprehensive knowledge of the status and intentions of both adversary and friendly forces across the air, land, sea, and space components of the battlespace. A concept labeled the Global Information Grid (GIG) will provide the network-centric environment required to achieve this goal.

The GIG will be a globally interconnected, end-to-end set of information capabilities, associated processes, and people to manage and provide information on demand to warfighters, policy makers, and support personnel.[3] While this "System-of-Systems" promises revolutionary

advances in information collection, processing and dissemination, it also has the potential to create and expose critical vulnerabilities that may be susceptible to catastrophic asymmetric attack. The Department of Defense (DoD) must ensure that the security of the GIG is based on a strategy that results from forethought rather than afterthought. Computer Network Defense (CND) policy, organization and technology development need to be fully integrated into the GIG infrastructure as it grows in size and complexity to ensure critical vulnerabilities are identified, minimized or eliminated before hostile exploitation can occur. Unfortunately, U.S. Defense Planning and, in particular, the policymaker's concept of national security have not caught up with, nor taken into account, the enormous changes required in information infrastructure protection imposed by this Revolution in Military Affairs (RMA). Rather, DoD thinking is fixated on forcibly fitting the critical role of CND into a pre-Internet construct premised on fighting the Cold War.

The UCP change that assigned responsibility for CND to U.S. Space Command (USSC) is a fundamentally flawed attempt to correct a perceived deficiency in Information Operations (IO) doctrine and organizational design. The CND mission has been defined too narrowly and rigidly and will result in the introduction of exploitable vulnerabilities in the Defense Information Infrastructure (DII). These DII vulnerabilities will be easily and quickly exploited by sophisticated adversaries in a manner that is imperceptible to those charged with protecting it. USSC will not and cannot be effective in improving the integration of CND into military planning and operations. On the contrary, it will likely slow development and fielding of new defensive capabilities, unnecessarily complicate inter-service and inter-agency coordination,

and potentially weaken the U.S. military's information security posture. An examination of current threats to the DII clearly shows that the level of effort required to protect the integrity of the GIG far exceeds the capability of USSC to execute its CND responsibilities in a manner consistent with UCP direction.

The Threat

> The reality seems compelling. At some future time, the United States will be attacked, not by hackers, but by a sophisticated adversary using an effective array of information warfare tools and techniques. Two choices are available: adapt before the attack or afterward.
>
> ----- Defense Science Board Task Force on Defensive Information Operations – 2000 Summer Study [4]

To date, there has been no comprehensive threat assessment performed of national, governmental or DoD information infrastructures and their vulnerability to attack. National Intelligence Estimates (NIE) are not sufficient in terms of fidelity or scope to form a basis for a comprehensive, fully integrated and detailed information assurance strategy. It is not sufficient to provide a general overview of postulated threat capabilities. The degree of vulnerability of the DII is a direct function of an adversary's capability to exploit its inherent security weaknesses. The greater the capability, the more critical the vulnerability. This process of evaluating threats and vulnerabilities is known as threat modeling. Too many consider security design a cookbook: mix in threat countermeasures such as intrusion detection, firewalls and encryption and magically, the system is secure. A sound security cycle or process begins with threat modeling then proceeds to development of security policy which, in turn, identifies an appropriate security solution.[5]

A sophisticated adversary will conduct computer network attack against the DII with the intention of achieving an operational or strategic objective(s). It will require detailed intelligence, a technology research and development capability, precise modeling and simulation, the ability to perform environmental preparations or social engineering, and target system-unique tactics, techniques and procedures (TTP). Does a potential adversary possess such an instrument and, if so, under what circumstances would such a capability be employed and for what purpose? These are difficult questions but ones that must be continuously assessed in order to implement and sustain a CND strategy that will be effective in ensuring the integrity of the DII.

The U.S. military is by far the most powerful military force that has ever existed in history. No nation state would dare risk a conventional frontal military assault against us. As a result, potential adversaries search for weaknesses around the edges in an attempt to identify critical vulnerabilities that may be exploited and attacked in an asymmetric manner. U.S. military forces are increasingly reliant upon information and information systems to maintain and extend its advantage in information superiority. In fact, the U.S. is far more reliant on information technology than any other nation. This makes it a target for computer-network attack since many if not most of its capabilities are inextricably linked to some form of automation of its information based processes. It is envisioned that virtually all forms of digital technology will eventually touch the GIG in some respect or another. Add to this, a propensity to quickly refresh these weapons, logistics and command and control (C2) systems with the latest commercially available technology, the growing sophistication of readily available CNA tools, the increasingly complex and interconnected nature

of the GIG itself, and the reliance of the GIG on commercial backbones to move information and it becomes abundantly clear that the possibility for the existence of critical vulnerabilities is significant.

A sophisticated threat will have little difficulty in accessing the DII in the accomplishment of a wide range of military objectives. During the three year period 1999 – 2001, National Security Agency (NSA) red teams conducted 27 assaults on DoD networks. Ninety-nine percent of these attacks went undetected even though the attacker used tools known by the network operator to exist (read – unsophisticated).[6] With this in mind, it can be reasonably assumed that a nation that has the capability to build a nuclear device or a ballistic missile would certainly have the wherewithal to cobble together a capability at least comparable to that of a NSA red team. In the absence of a comprehensive national threat assessment, this should serve as the threat model on which to base DII CND strategy. Current DoD security strategy, based on anecdotal information describing tactics used by unsophisticated would-be interlopers, grossly underestimates the magnitude, maturity, and determination of the menace arrayed against it. It almost certainly places the integrity of the DII in jeopardy and, with it, elements of U.S. National Security.

The Mission of Computer Network Defense

> The fact is that we are currently building an information infrastructure -- the most complex systems the world has ever known -- on an insecure foundation. We have ignored the need to build trust into our systems. Simply hoping that someday we can add the needed security before it is too late is not a strategy.
>
> ----- George J. Tenet, Director of Central Intelligence, April 1998.[7]

CND are defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction.[8] It is a very broad mission that, to be successful, must be fully integrated throughout the entire military force. The whole notion of security in a networked environment is based on the principle of “shared risk.” That is to say, risk taken by one entity on the network is shared by all that are connected to it. Risk can be introduced at virtually any point in time, at any place, and in many forms ranging from initial architectural design considerations to

the adjudication of personnel security clearances. Consequently, the integration of CND throughout the entire military force translates to a top-to-bottom, end-to-end, and cradle-to-grave capability. Today, the DII, primarily consisting of the Nonsecure Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET), is vulnerable to a wide range of sophisticated and unsophisticated threats. The DII consists of over 3 million host computers on 10,000 networks running several different operating systems and more than 700 applications – all collectively requiring in excess of 100 million lines of code. It is operated by approximately 125,000 system administrators.[9] DoD relies on the DII to move 95 percent of its communications traffic. Seventy percent of traffic traversing the NIPRNET flows to and from the Internet.[10] While the SIPRNET is not directly connected to the Internet, it is connected to the NIPRNET through a variety of Secret and Below Interoperability (SABI) interfaces. Additionally, the Joint Worldwide Intelligence Communications System (JWICS) is connected to the SIPRNET through interface technology referred to as High Assurance Guards (HAGs). These interfaces can be critically important considering that any boundary that allows data to flow through it is vulnerable to a data driven attack.[11] The DII continues to grow in scope and complexity with each passing day as evidenced by interest in major new Service initiatives. The Navy is in the process of implementing its 7 billion dollar Navy/Marine Corps Intranet (NMCI) and the Army and Air Force are studying similar initiatives.[12]

The DoD strategy for providing Information Assurance (IA) in this rapidly growing information infrastructure is a concept called Defense in Depth (DID) DID is advertised to achieve multi-layer, multi-dimensional protection through the integration of the capabilities of

people, operations and technology. The thought is that constructing successive layers of protection will cause an adversary who penetrates or breaks down a barrier to promptly encounter another DID barrier, and another, and another until the attacker's capabilities are exhausted or his activities are detected and effectively countered. Further, to counter different attack methods, a corresponding variety of security methods are employed. The weaknesses of one safeguard mechanism should be balanced by the strengths of another. DID focuses on local computing environments or enclaves, enclave boundaries, networks that link enclaves, and supporting infrastructure. It is clear that the objective of DID is, or at least should be, identical to that of CND.[13] Regardless of what one calls the process of protecting the DII, the real question remains, is it secure? The following scenario might be useful in answering this question:

> On 13 October 2004, after showing his military identification, Operations Specialist First Class Smith drives his car through the front gate of a DoD installation located in the Washington D.C. area. After navigating his car through the obstacle course of concrete barriers at the entrance of the parking lot he is required to show his organization-issued security badge to a contract security guard who briefly glances at the DoD sticker on his window and then ensures his face matches the badge picture before waving him through. With briefcase in hand, he quickly walks through the front doors of the building where he works and into the main lobby. Under the watchful eye of another security guard, Petty Officer Smith inserts his security badge into the badge reader and punches in his four digit Personal Identification Number (PIN). The reader verifies his identification and allows him

to pass through the turnstile. Upon reaching his workspace, he must remember yet another 4 digit code to open the cipher lock on the front door. He sits down at his desk and types his logon and password into his newly installed computer. Just before leaving his desk for lunch, Petty Officer Smith reaches into his briefcase and removes a Read/Write DVD and inserts into his computer. Returning from lunch he removes the DVD and puts it back into his briefcase. At 1600, he leaves for the day departing in the same manner in which he had arrived. Later that night, he places the DVD into a preaddressed envelop and slips it into the mail. Petty Officer Smith has arguably just committed the gravest act of espionage in U.S. history.

Using a slightly modified web browser application and a dictionary of key word search strings, the DVD searched a classified DoD computer network for specific information, downloaded in excess of five gigabytes of information, mapped the network's infrastructure and established presence on a number of systems resident on the network. This scenario gives some insight into just how easily and quickly a witting insider can cause catastrophic damage to the entire DII. Each of the 2 million DII users are potential targets for a sophisticated adversary. Success requires that only one user be effectively engaged. This is the soft underbelly of the DII. The biggest challenge confronting security managers in today's information environment is the ability to access huge volumes of information coupled with the ability to store it on a medium that is easily concealed and transported. Sophisticated adversaries using witting and unwitting insiders pose an enormous threat to national security and a monumental challenge to DoD information security resources. These challenges have not been adequately addressed by the DID strategy let alone USSC CND efforts. USSC cannot and will not provide the comprehensive capability to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction across the broad threat spectrum the DoD currently faces. Mr. Arthur Money, Assistant Secretary of Defense for Command, Control, Communications and Intelligence (C3I), admitted as much saying "We want to move from a Defense in Depth to a

Defense in Breadth. . . This involves looking across a broader spectrum of potential attacks, including those of cooperative insiders."[14] This is an admission that the current approach is inadequate for the task that lies ahead or, for that matter, the one at hand. The current strategy and, in particular, the CND component concentrate on providing DID around enclave boundaries much like a fence or series of fences instead of interweaving security features throughout the breadth of the enclaves in manner that guarantees continuous surveillance and evaluation of user-operator activities. This type of protection has to be built into systems and not added on after production and installation.

U.S. Space Command and CND

In 1997, a series of exercises and real-world events targeted at DoD networks demonstrated that critical DoD information and information systems were exposed to unacceptable risk of exploitation and attack. While many organizations in DoD were keeping pace with technological developments in the field of information security, there was no single organization that was charged with coordinating defensive actions across the entire department. Early the following year, it had become apparent that the DoD required a new organizational approach to pull together various information assurance resources in a manner that facilitated unity of effort in coordinating the defense of computer networks and exercising needed operational authority to direct the actions necessary for that defense. At the time, there was general agreement one of the Department's nine Combatant Commands would be assigned this mission. However, the time needed to staff and implement such a decision required that an interim solution be implemented while awaiting the formal UCP process to take its course. The agreed upon interim solution was to establish the Joint Task Force for Computer Network Defense (JTF-CND) in December 1998.[15]

On 1 October1999, UCP 99 assigned new CND responsibilities to USSC. In response to the growing threat to U.S. military information systems and the military's increasing reliance on these systems to perform its mission, the UCP assigned USSC as "the military lead for CND and, effective 1 October 2000, CNA, to include advocating the CND and CNA requirements of all CINCs, conducting CND and CNA operations, planning and developing national requirements for CND and CNA, and supporting the other CINCs for CND and CNA."[16] It goes on to say that this is intended as just an initial step to ensure the DoD is prepared to exploit its strategic information advantage. While USSC

assumes the two IO responsibilities of CND and CNA, it leaves other IO responsibilities such as Electronic Warfare, Military Deception, Operations Security, Physical Destruction, Information Assurance and Psychological Operations to be addressed within the current command structure by the appropriate CINCs, Services or defense agencies. Indeed, the document argues that CND and CNA are of such paramount importance that, in addition to requiring new CINC level attention, it "envisions the possibility of a fundamental reorientation of USSC resulting in the formation of a Space and Information Command."[17]

Since being assigned these responsibilities, USSC has assumed operational control of Joint Task Force – Computer Network Operations (JTF-CNO). As USSC's operational component for CNO, the mission of JTF-CNO is to coordinate and direct the defense of DoD computer systems and networks: coordinate and, when directed, conduct computer network attack in support of CINC's and national objectives. USSC views its CND mission as defending DoD computer networks and systems from any unauthorized event whether it be a probe, scan, virus incident, or intrusion.[18] This seems even broader in scope than the DoD definition of CND as defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction. Although not explicitly stated in the above mission statement, preventing intrusion into DoD information systems for the purpose of espionage is implied. According to Lt. Col. John Pericas, USAF, chief officer for computer network defense operations, USSC, the idea is to simultaneously protect and facilitate defense information system network activities so that both defensive and offensive measures can be maximized to support mission success. "With this two-pronged approach, we not only defend our data from threats that would steal it, but project our own capabilities to disrupt enemy operations."[19]

General Henry H. Shelton, Chairman of the Joint Chiefs of Staff, provided insight into why USSC was chosen when he said that USSC was a logical fit given its global perspective and its collection of experts adept at operating computers, communications systems, and space assets.[20] The connection drawn by General Shelton between operating computers and CND is tenuous at best. CND is a capability that requires specialized skills, technology and TTP. There are other organizations within the DoD that have far greater expertise in CND than USSC while also offering a

global perspective. The National Security Agency (NSA) is one example. Lt. General Edward Anderson III, Deputy Commander in Chief, U.S. Space Command provided additional insight into USSC's envisioned role when he wrote, "USSC's strategic objective is to operationalize CNO into the fifth domain of warfare, separate and distinct, but fully integrate it into air, land, sea, and space across the full spectrum of conflict with the ability to leverage the computer network domain to achieve and maintain information and decision superiority for the joint force. To achieve this, USSPACECOM has developed a multiphased CNO campaign plan to direct the planning, operational, technical, and programmatic integration activities to operationalize CNO."[21] Essentially, the current USSC strategy is to combine CNA and CND under a single command to establish unity of effort, conserve resources and improve cross-agency coordination with the objective of operationalizing CNO. In this context, the term "operationalize" is taken to mean the integration of people, technology and TTP in such a manner so as to establish adequate protection for the information and information systems that are required to plan and conduct military operations.

Can U.S. Space Command Operationalize CND?

Today, USSC is in the process of actually defining exactly what it is they should be doing. Indeed, Lt. General Anderson stated "This is not something where we can open up some books or open up some file folders and see how it used to be done, because basically, it is a new task for the military."[22] This implies that CND has not previously existed at the operational level. This is simply incorrect. DoD Services and Agencies have been evolving CND technologies, policies, procedures, training and awareness long before USSC assumed its CND responsibilities. What is not at all clear are the benefits USSC brings to the CND table.

The idea of creating unity of effort by combining CNA and CND to form CNO and placing it under the control of a single commander is a red herring. The first element in building a case for CNO unity of effort is the creation of synergy. It assumes the skills, technology and techniques required to conduct CNA operations against an adversary's information systems are interchangeable with those an adversary would use to attack DoD information systems and, therefore, the CND mission would benefit from knowledge of own force CNA capabilities. In reality, the skills, technology and techniques required to successfully attack foreign military information enclaves are vastly different from

those required to attack the DII. General Richard Myers, Commander in Chief, U.S. Space Command, said the Pentagon considered employing CNA in Kosovo but the opportunities were limited because the Serbian military forces were not heavily dependent on information systems.[23] Certainly, Serbian military forces were dependent on information systems.[24] The point the General was probably attempting to make was that Serbian information systems were not networked commercial-off-the-shelf (COTS) based systems connected to the Internet as are U.S. military information systems. Accordingly, no access point had been developed, there was little intelligence concerning system specifications or operating procedures, and CNA tools had not been developed, tested, or deployed. This is the reality minus the mirror imaging.

The second augment used in building a case for CNO unity of effort involves the use of CNA as a possible response option associated with CND operations. In this scheme, CNA would be used to compel an attacker to cease hostile or disruptive cyber activity against the DII. The requirement to establish positive identification of the intruder for the purpose of counterattack is impracticable in terms of legal constraints, technical limitations and attack preparation time. Even in the highly unlikely event that all of the legal and technical issues could be surmounted in a reasonable timeframe, the chance of imparting damage on a scale that would be of any deterrence value is negligible.

The centerpiece of USSC's effort to operationalize CND, the JTF-CNO (formerly JTF-CND), has been operational for four years, an eternity in the information security world. Yet, from a CND perspective, the JTF-CNO, is still focused on gathering information, coordinating incident reporting, and performing analysis on low-level, hacker related events. The outlook for this changing any time in the near future is less than optimistic. For example, General Eberhart views the JTF-CNO as a "pathfinder" organization that will adapt to changing threats and mission parameters.[25] Once again, the organization has done little in the past four years to positively impact the ability of the DoD to effectively address the sophisticated CNA threats it currently faces.

It is widely acknowledged that the intrusion detection technology currently used as the primary tool by the JTF-CNO to detect computer network attacks is ineffectual against a hacker of even modest talents as evidenced by results from numerous NSA red team exercises. One can only wonder where a "pathfinder" organization that has operated for

four years, spent millions of dollars and is still unable to effectively address the most basic of all cyber threats is leading the Department. Consider the damage inflicted by the Love Bug virus which infected unclassified DoD networks worldwide as well as a few classified systems. This is a virus that was created with 50 lines of basic code written by a couple of students in the Philippines.[26] Just think what could have been accomplished had a sophisticated adversary wanted to infect and take down the DII. The DoD is proceeding down the road that George Tenet spoke of four years earlier. Namely, building the DII on an insecure foundation, ignoring the need to build trust into its information systems, and hoping that someday the needed security can be added before it is too late. The assignment of CND responsibilities to an organization that does not have the authority or capability to ensure trust is built into DoD information systems has only exacerbated the problem. This is particularly disconcerting as DoD capability to defend the DII fails to keep pace with the increasingly sophisticated CNA tools available in the public domain. Representative Stephen Horn, Chairman of the House Government Reform Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations assigned the DoD an overall grade of "F" in computer security for FY 2001 based on Office of Management and Budget reports and General Accounting Office audits. This is down from a D+ in FY 2000.[27] The fact is the DoD has vastly misjudged the scale and sophistication of the threat it is facing. Consequently, the entire premise upon which the USSC CND organizational construct is based is an illusion.

The goal of USSC's multiphased campaign plan is admirable. However, the USSC does not possess the expertise, resources or authority to implement it, nor should they. In essence, USSC is proposing a strategy for manning, training and equipping forces to conduct CND. This directly impinges on the Services Title 10 responsibilities to man, train, and equip their own forces. As discussed above, in order to conduct effective CND operations in a shared risk environment, the effort must be comprehensive in nature, that is, end-to-end, top-to-bottom and cradle-to-grave. The vast majority of this responsibility resides at the service level. Geographical CINCs have every right to expect that when a platform or system is deployed to their theater of operation, adequate CND protective measures have been implemented doctrinally, procedurally, technologically, and embedded in the training of the sailors, soldiers and airmen who operate it. In point of fact, USSC will never have the authority to implement, coordinate, or manage a comprehensive CND strategy.

The initial UCP assignment of CND responsibilities to USSC was fatally flawed by leaving the responsibility for IA with the Services. Recall, CND is defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction while IA is actions that protect and defend information and information systems by ensuring availability, integrity, authentication, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities .[28] Just what is one without the other? This is analogous to removing physical security from force protection or infectious diseases from medicine and placing them under the auspices of a functional CINC because of a growing concern about terrorism. Separating the two functions can only result in fracturing any hope of achieving unity of effort. The preponderance of evidence leaves little doubt that responsibility for CND must reside with IA and its strategic implementation concept of DID. It is also evident that without the adoption of a comprehensive CND strategy, significant security vulnerabilities will be inherent in the GIG and have a deleterious effect on the implementation of NCW.

The JTF-CND/CNO experiment of the past four years has conclusively proven itself to be the wrong organizational construct to provide DoD Indications & Warning (I&W) of potential hostile or malicious computer network activity. The Department would be better served by considering one of the combat support agencies such as the NSA to perform the I&W function. They have the requisite technical expertise, well established inter-service and interagency relationships, and analytic capabilities to effectively and efficiently perform this function.

The DoD cannot operationalize CND by playing the shell game of reorganization. Any serious endeavor to improve network security will require uncomfortable and unpopular decisions concerning tradeoffs between information system functionality and the information security architecture. Today, most of these decisions are made in favor of improving functionality at the expense of security. This is not surprising. With no detailed assessment of threat, operational level decision makers have little basis on which to assess risk and, therefore, naturally dismiss potential adverse security consequences as remote or unlikely. This approach has left the soft underbelly of the DII exposed to enormous dangers from witting insider attacks, user-operator foibles, sophisticated data driven exploitation, and infestation by relatively unsophisticated malicious code. Information security policy, TTP, and technology must derive

from an assessment based on the threat posed by a sophisticated adversary and be comprehensively integrated throughout the information environment and not just at enclave boundaries. Protecting the shared risk environment of the GIG demands absolute compliance with IA guidance and direction even it requires disconnecting "mission critical" systems, revoking or reducing access, removing functionality, or terminating programs.

No, the U.S. Space Command cannot operationalize CND. CND, in large measure, consists of a level of trust that must be trained into people, build into systems, and integrated into networks. It is not a blanket of protection that can be thrown over a capability as it enters service or a theater of operations.

Conclusion

The Congress, the Defense Science Board, and the Assistant Secretary of Defense for C3I have all stated or, at least, strongly implied that the current strategy for protecting the DII and GIG is intolerable. The DoD no longer has the luxury of continuing to "bet the farm" on a strategy which could result in significant damage to National Security. It is incumbent on the Services to ensure the integrity of their information enclaves as a function of their Title 10 responsibilities. Organizationally, they are the only ones who can implement the degree of comprehensive network security required to effectively defend against a sophisticated adversary. DoD information enclaves, either viewed individually or collectively as a system of systems, are interconnected information technologies that are built, fielded, maintained and operated by service components. Assigning responsibility for their protection, either in part or in full, to an organization other than the appropriate Service cannot succeed.

Information security is not a technology, a skill, or a policy. It is the process of identifying the right security solution with forethought and building it into the DII from the beginning. Responsibility for this process lies primarily with the Services. The DoD is at what Andrew Grove, Chairman of the Board, INTEL Corp., called a strategic inflection point.[29] The path chosen may well forecast the future of Network Centric Warfare. DoD needs to show the courage and wisdom to choose well.

Notes

[1] Defense Science Board, Protecting the Homeland, Report of the Defense Science Board Task Force on Defensive Information Operations – 2000 Summer Study Volume II (Washington, D.C., March 2001), ES-1.

[2] U.S. Joint Chiefs of Staff. Information Assurance Through Defense in Depth (Washington, D.C., 2000), 2.

[3] Martin Libicki, Who Runs What In the Global Information Grid: Ways To Share Local and Global Responsibility (Santa Monica, CA: RAND, 2000), ix.

[4] Defense Science Board, Protecting the Homeland, ES-1.

[5] Bruce Schneier, Secrets and Lies: Digital Security in a Networked World (New York, NY: John Wiley & Sons, 2000). 302-303

[6] Defense Science Board, Protecting the Homeland, ES-4.

[7] George J. Tenet, Director of Central Intelligence, Remarks on Information Security Risks, Opportunities, and the Bottom Line before the Sam Nunn Nations Bank Policy Forum, Atlanta, GA, 06 April 1998. 1.

[8] U.S. Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, Joint Pub 1-02 (Washington, D.C.: 12 April 2001), 89.

[9] Defense Science Board, Protecting the Homeland, ES-2.

[10] Major General James D. Bryan, USA, Commander, Joint Task Force-Computer Network Operations, U.S. Space Command and Vice Director, Defense Information Systems Agency, on Protection of Computer Networks before the House Armed Services Committee, Washington D.C., 17 May 2001. 3.

[11] Data driven attack: A cyber attack carried out by maliciously encoding a seemingly innocuous piece of data that is not recognized as malicious and, therefore, allowed to pass through a security boundary such as a firewall. Upon penetrating the enclave boundary, an unwitting insider executes the malicious code.

[12] Frank Tiboni, "U.S. Army Considering NMCI-Like Computer Network," DefenseNews.com, 30 April 2002, <http://ebird.dtic.mil/May2002/s20020502considering.htm>, [02 May 2002]

[13] U.S. Joint Chiefs of Staff. Information Assurance Through Defense in Depth, (Washington, D.C.: February 2000), 6.

[14] Robert K. Ackerman, "Jointness defines priorities for the defense department's global grid," Signal (April 2001) 23-27.

[15] Major General James D. Bryan, USA, Commander, Joint Task Force-Computer Network Operations, U.S. Space Command and Vice Director, Defense Information Systems Agency, on Protection of Computer Networks before the House Armed Services Committee, Washington D.C., 17 May 2001, 1.

[16] Office of the President of the United States, Unified Command Plan (S). 13 SEP 1999. 15. Quote comes from unclassified paragraph.

[17] Office of the President of the United States, "Unified Command Plan Vision 21," Unified Command Plan (S), Encl. 1, 13 SEP 1999. 4.

[18] U.S. Space Command, Fact Sheet, <http://www.spacecom.mil/history.htm> [3 May 2002].

[19] Christian B. Sheehy, "Space Warriors Defend Information Assets," Signal, April 2001, Proquest, Ann Arbor, MI: Bell & Howell Information and Learning Company, [21 March 2002].

[20] Michael C. Sirak, "Threats to the Nets," Air Force Magazine Online, Vol. 84, No.10, October 2001, 3. <http:/www.afa.org/magazine/Oct2001/1001network.html>, [23 March 2002]

[21] Lt. General Edward G, Anderson III, U.S. Army, Deputy Commander in Chief and Chief of Staff, U.S. Space Command, "U.S. Space Command:Warfighters supporting warfighters in the 21st century," Military Review, November/December 2001, 6.

[22] Michael C. Sirak, "Threats to the Nets," 2.

[23] Paul Stone, "Space Command Plans for Computer Network Attack Mission." SpaceDaily, Washington, D.C., 11 January 2000, <http://www.spacedaily.com/news/milspace-00a.html>, [07 May 2002].

[24] Information System**:** The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. Joint Publication 1-02, "DoD Dicitionary of Military and Associated Terms," April 2001, 209.

[25] General Ralph E. Eberhart, USAF, Commander in Chief Untied States Space Command, 11.

[26] Arnaud de Borchgrave, Frank J. Cilluffo, Sharon L. Cardash, and Michele M. Ledgerwood, "Cyber Threats and Information Security – Meeting the 21st Century Challenge," Center for Strategic International Studies (Washington, D.C., December 2000), v.

[27] Joshua Dean, "Feds get 'F' in computer security." GovExec.com, 09 November 2001, <http://www.govexecc.com/dailyfed/1101/110901j1.htm>, [08 May 2002].

[28] U.S. Joint Chiefs of Staff. Information Assurance Through Defense in Depth, 2.

[29] Strategic inflection point: A time in the life of a business when its fundamentals are about to change. That change can mean an opportunity to rise to new heights. But it may just as likely signal the beginning of the end. Andrew Grove, Only the Paranoid Survive (New York, Random House, 1999), Preface.

Bibliography

Ackerman, Robert K., "Jointness defines priorities for the defense department's global grid," Signal, April 2001.

Alberts, David S., and John J. Garstka, Frederick P. Stein. Network Centric Warfare – Developing and Leveraging Information Superiority. 2nd ed. (Revised). Washington D.C.: Department of Defense C4ISR Cooperative Research Program, 2000.

Alberts, David S., Defensive Information Warfare. Washington, D.C.: National Defense University, 1996.

Anderson, Robert H., Richard Brackney, and Thomas Bozek. "Advanced Network Defense Research." Proceedings of Workshop. Santa Monica, CA: RAND, 2000

Arquilla, John, David Ronfeldt, and Michele Zanini. "Netwar, and Information Age Terrorism." The Changing Role of Information in Warfare, edited by Zalmay M. Khalilzad and John P. White. Santa Monica, CA: RAND, 1999.

Arquilla, John, David Ronfeldt. "The Emergence of Noopolitik: Toward an American Information Strategy." Santa Monica, CA: RAND, 1999

Barnes, Robert C. "Improving the Unified Command Plan for the 21st Century." Unpublished Research Paper, U.S. Army War College, Carlisle Barracks, PA: 2000.

Barnett, RogerW. "Information Operations, Deterrence, and the Use of Force." Naval War College Review. Spring 1998.

Borchgrave, Arnaud de., Frank J. Cilluffo, Sharon L. Cardash, and Michele M. Ledgerwood. "Cyber Threats and Information Security: Meeting the 21st Century Challenge." Washington D.C.: Center for Strategic and International Studies, December 2000.

Bryan, Major General James D., USA, Commander, Joint Task Force-Computer Network Operations, U.S. Space Command and Vice Director, Defense Information Systems Agency, On Protection of Computer Networks before the House Armed Services Committee, Washington D.C., 17 May 2001.

Bush, George W. "Critical Infrastructure Protection in the Information Age." Executive Order. The White House: 16 October 2001.

Chaisson, Kernan. "Cyber offensive mission to begin." Journal of Electronic Defense. March 2000. ProQuest. Ann Arbor, MI: Bell & Howell Information and Learning Company. [10 March 2002].

_____. "Cyber Warfare Rules 'Bumfuzzle' DOD Lawyers." Journal of Electronic Defense. January 2000. ProQuest. Ann Arbor, MI: Bell & Howell Information and Learning Company. [10 March 2002].

Clausewitz, Carl von. On War. Michael Howard and Peter Paret eds. and trans. Princeton: Princeton University Press, 1984.

Clinton, William J. A National Security Strategy for a Global Age. Washington D.C.: The White House, December 2000.

_____. National Security Science and Technology Strategy. . Washington D.C.: The White House, October 1998.

_____. National Plan for Information Systems Protection. Washington D.C.: The White House, January 2000

_____. The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. White Paper. Washington D.C. 22 May 1998.

Dean, Joshua, "Feds get 'F' in computer security." GovExec.com, 09 November 2001, <http://www.govexecc.com/dailyfed/1101/110901j1.htm>, [08 May 2002].

Defense Science Board. Protecting the Homeland: Report of the Defense Science Board on Defensive Information Operations – Summer Study 2000 Volume II. Washington, D.C.: Office of the Under Secretary of Defense for Acquisition and Technology, March 2001.

Defense Science Board. Report of the Defense Science Board Task Force on Information Warfare – Defense. Washington, D.C.: Office of the Under Secretary of Defense for Acquisition and Technology, November 1996.

Denning, Dorothy E. Information Warfare and Security. Reading, MA: Addison – Wesley, 1999.

Gruber, David J. “Computer Networks and Information Warfare – Implications for Military Operations.” Occasional Paper No. 17. Center for Strategy and Technology, Air War College: 2000.

Libicki, Martin, Who Runs What In the Global Information Grid: Ways To Share Local and Global Responsibility. Santa Monica, CA: RAND, 2000

Molander, Roger C., Peter A. Wilson, David A. Mussington, Richard F. Mesic, Strategic Information Warfare Rising. Santa Monica, CA: RAND, 1998.

Molander, Roger C., Peter A. Wilson, and Robert H. Anderson. “U.S. Strategic Vulnerabilities: Threats Against Society.” The Changing Role of Information in Warfare, edited by Zalmay M. Khalilzad and John P. White. Santa Monica, CA: RAND, 1999.

Office of the President of the United States, 1999 Unified Command Plan and UCP 21 Vision. JCS Document MCM-162-99 Washington, D.C.: Department of Defense, 13 October 1999.

Patterson, Christina M. Lights Out and Gridlock: The Impact of Urban Infrastructure Disruptions on Military Operations and Non-Combatants. Alexandria, VA: Institute for Defense Analyses, September 2000.

Schneier, Bruce. Secrets and Lies: Digital Security in a Networked World. John Wiley & Sons. New York, NY: 2000.

Schutze, James T. Defensive Information Operations – An Interagency Process. Unpublished Research Paper, U.S. Army War College, Carlisle Barracks, PA: 2001.

Sheehy, Christian B., “Space Warriors Defend Information Assets,” Signal, April 2001, Proquest, Ann Arbor, MI: Bell & Howell Information and Learning Company, [21 March 2002].

Sirak, Michael C., “Threats to the Nets,” Air Force Magazine Online, Vol. 84, No.10, October 2001, <http:/www.afa.org/magazine/Oct2001/1001network.html>, [23 March 2002]

Smith, Edward A., Jr. “Network-Centric Warfare: What’s the Point?” *Naval War College Review* (Winter 2001).

Stone, Paul, “Space Command Plans for Computer Network Attack Mission.” SpaceDaily, Washington, D.C., 11 January 2000, <http://www.spacedaily.com/news/milspace-00a.html>, [07 May 2002].

Tenet, George J. Director of Central Intelligence, Remarks on Information Security Risks, Opportunities, and the Bottom Line before the Sam Nunn Nations Bank Policy Forum, Atlanta GA, 06 April 1998.

Tiboni, Frank, DefenseNews.com, U.S. Army Considering NMCI-Like Computer, 30 April 2002, <http://ebird.dtic.mil/May2002/s20020502considering.htm>, [02 May 2002]

U.S. Department of Defense Office of General Counsel. "An Assessment of International Legal Issues in Information Operations." 2nd Edition, November, 1999.

U.S. Joint Chiefs of Staff. Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations (Joint Pub 6-0) Washington, D.C.: 30 May 1995

U.S. Joint Chiefs of Staff. Doctrine for Joint Operations. (Joint Pub 3-0) Washington, D.C.: 10 September 2001.

U.S. Joint Chiefs of Staff. Doctrine for Intelligence Support to Joint Operations (Joint Pub 2-0) Washington, D.C.: 9 March 2000.

U.S. Joint Chiefs of Staff. Joint Doctrine for Command and Control Warfare (Joint Pub 3-13.1) Washington, D.C.: 7 February 1996.

U.S. Joint Chiefs of Staff. Joint Doctrine for Information Operations (Joint Pub 3-13) Washington, D.C.: 9 October 1998.

U.S. Joint Chiefs of Staff. Joint Warfare of the Armed Forces of the United States (Joint Pub 1) Washington, D.C.: 14 November 2000.

U.S. Joint Chiefs of Staff. Joint Vision 2010. Washington, D.C.: U.S. Government Printing Office, 1995.

U.S. Joint Chiefs of Staff. Joint Vision 2020. Washington, D.C.: U.S. Government Printing Office, June 2000.

U.S. Joint Chiefs of Staff. History of the Unified Command Plan, 1946-93. Washington, D.C.: U.S. Government Printing Office, 1995.

U.S. Joint Chiefs of Staff. Information Assurance Through Defense in Depth. Washington, D.C.: U.S. Government Printing Office, 2000.

U.S. Joint Chiefs of Staff. Information Operations – A Strategy for Peace: The Decisive Edge in War. Washington, D.C.: U.S. Government Printing Office, 1999.

U.S. Joint Chiefs of Staff. National Military Strategy of the United States of America – Shape, Respond, Prepare Now: A Military Strategy For a New Era. Washington, D.C.: U.S. Government Printing Office, 1997.

U.S. Space Command, Fact Sheet, <http://www.spacecom.mil/history.htm> [3 May 2002].